

# CYBERSECURITY RECOMMENDATIONS FOR THE NEXT ADMINISTRATION

---

## HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING  
THREATS, CYBERSECURITY,  
AND SCIENCE AND TECHNOLOGY

OF THE

COMMITTEE ON HOMELAND SECURITY  
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

SEPTEMBER 16, 2008

**Serial No. 110-138**

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpoaccess.gov/congress/index.html>

U.S. GOVERNMENT PRINTING OFFICE

48-089 PDF

WASHINGTON : 2009

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

## COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California	PETER T. KING, New York
EDWARD J. MARKEY, Massachusetts	LAMAR SMITH, Texas
NORMAN D. DICKS, Washington	CHRISTOPHER SHAYS, Connecticut
JANE HARMAN, California	MARK E. SOUDER, Indiana
PETER A. DEFAZIO, Oregon	TOM DAVIS, Virginia
NITA M. LOWEY, New York	DANIEL E. LUNGREN, California
ELEANOR HOLMES NORTON, District of Columbia	MIKE ROGERS, Alabama
ZOE LOFGREN, California	DAVID G. REICHERT, Washington
SHEILA JACKSON LEE, Texas	MICHAEL T. MCCAUL, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands	CHARLES W. DENT, Pennsylvania
BOB ETHERIDGE, North Carolina	GINNY BROWN-WAITE, Florida
JAMES R. LANGEVIN, Rhode Island	GUS M. BILIRAKIS, Florida
HENRY CUELLAR, Texas	DAVID DAVIS, Tennessee
CHRISTOPHER P. CARNEY, Pennsylvania	PAUL C. BROUN, Georgia
YVETTE D. CLARKE, New York	CANDICE S. MILLER, Michigan
AL GREEN, Texas	
ED PERLMUTTER, Colorado	
BILL PASCRELL, JR., New Jersey	

I. LANIER LAVANT, *Staff Director*

ROSALINE COHEN, *Chief Counsel*

MICHAEL TWINCHEK, *Chief Clerk*

ROBERT O'CONNOR, *Minority Staff Director*

---

## SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY

JAMES R. LANGEVIN, Rhode Island, *Chairman*

ZOE LOFGREN, California	MICHAEL T. MCCAUL, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands	DANIEL E. LUNGREN, California
BOB ETHERIDGE, North Carolina	GINNY BROWN-WAITE, Florida
AL GREEN, Texas	PAUL C. BROUN, Georgia
BILL PASCRELL, JR., New Jersey	PETER T. KING, New York ( <i>Ex Officio</i> )
BENNIE G. THOMPSON, Mississippi ( <i>Ex Officio</i> )	

JACOB OLCOTT, *Director and Counsel*

DR. CHRIS BECK, *Senior Advisor for Science and Technology*

CARLA ZAMUDIO-DOLAN, *Clerk*

KEVIN GRONBERG, *Minority Professional Staff Member*

## CONTENTS

	Page
STATEMENTS	
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island, and Chairman, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology .....	1
The Honorable Michael T. McCaul, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology .....	5
The Honorable Ginny Brown-Waite, a Representative in Congress From the State of Florida: Prepared Statement .....	6
WITNESSES	
Mr. David Powner, Director, Information Management Issues, Government Accountability Office: Oral Statement .....	7
Prepared Statement .....	9
Mr. James A. Lewis, Project Director, Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies; Accompanied by Lieutenant General Harry D. Raduege, Jr., Co-Chairman, Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies; and Paul Kurtz, Member, Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies: Oral Statement .....	18
Prepared Statement .....	20
FOR THE RECORD	
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island, and Chairman, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology: Letter .....	4



## **CYBERSECURITY RECOMMENDATIONS FOR THE NEXT ADMINISTRATION**

---

**Tuesday, September 16, 2008**

U.S. HOUSE OF REPRESENTATIVES,  
COMMITTEE ON HOMELAND SECURITY,  
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND  
SCIENCE AND TECHNOLOGY,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 2:22 p.m., in Room 311, Cannon House Office Building, Hon. James R. Langevin [Chairman of the subcommittee] presiding.

Present: Representatives Langevin, Green, Pascrell, and McCaul.

Mr. LANGEVIN. The subcommittee will come to order. The subcommittee is meeting today to receive testimony on cybersecurity recommendations for the next administration. I will begin by recognizing myself for the purposes of an opening statement.

Of course I want to thank our panel for being with us today. Good afternoon, and welcome to our final public hearing of the 110th Congress. The Subcommittee on Emerging Threats, Cybersecurity, Science and Technology has tackled a number of critical issues related to our national security, including biological, chemical, agricultural, radiological, and nuclear threats. We have had an extremely busy schedule, and I thank all of the Members for their commitment and their leadership over the course of this Congress.

Today we are holding our eighth hearing on cybersecurity. I don't think anyone would disagree when I say that this subcommittee has established itself as the policy leader in the U.S. Congress on the issue. We have held hearings on hacking incidents at the Department of State, Commerce, and Department of Homeland Security; cyber attacks on our internet infrastructure; oversight on the Cyber Initiative; the need for additional investment in cybersecurity research and development; mitigating cyber vulnerabilities in the electric grid; DHS and critical infrastructure sector plans to mitigate cyber vulnerabilities; and incentives for private sector critical infrastructure owners to mitigate cyber vulnerabilities.

This is a significant number of hearings, but it is one thing to hold hearings and quite another to improve the security of America. That is our goal. That is what I want to talk about today. I believe our oversight has enhanced Federal and critical infrastructure cybersecurity by improving security at DHS, highlighting and filling gaps in Federal cybersecurity policy, and holding individuals in public and private sectors accountable.

First, we have improved situational awareness, increased security on networks at the Department of Homeland Security across

the Federal Government. Our goal on this committee, one that I have discussed on many occasions, is to make the Department of Homeland Security the gold standard in Federal information security. We have got a long way to go before we get there, however. But as a result of our investigations and hearings, the CIO's Office began receiving more threat briefings. That raises situational awareness.

The CIO also began working in a more collaborative fashion with US-CERT after we questioned why the EINSTEIN system wasn't deployed on more networks at DHS. Shortly after our June 2007 hearing, EINSTEIN was deployed at more than 2 dozen DHS gateways, providing greater insight into the significant number of attacks on Government systems. This helps us to know where to commit resources to our defenses.

Now, we also saw results from those early subcommittee hearings. In April 2007 we called for a national-level initiative that would standardize intrusion detection technologies across the Federal Government. Eight months later, the administration announced a new Cyber Initiative to improve the security posture of the Federal Government's networks.

Second, the subcommittee's oversight has filled and will continue to fill significant gaps that exist in Federal cybersecurity policy. We spent a significant amount of time on the electric grid, one of our most vulnerable critical infrastructure sectors. In 2007, this subcommittee initiated a review of the Federal Government's effort and ability to ensure the security of the bulk power system from cyber attack. We began surveying the electric sector to determine their mitigation efforts for the Aurora vulnerability. During my review of these efforts, it became evident that mitigation of this vulnerability was highly inconsistent. My colleagues and I were surprised and disturbed to see how dismissive many of the companies were of this vulnerability, so we began doing all we could to ensure that it would be fixed.

Today, because of our hearings, more companies are mitigating Aurora and other cyber vulnerabilities in their systems. During that review, we also identified inconsistent Federal policies that would leave the grid vulnerable to cyber attack.

Last week, I testified before the Energy and Commerce Subcommittee on Energy and Air Quality about the need to provide the Federal Energy Regulatory Commission with emergency authority to ensure the security of the electric system from cyber attack. I am highly optimistic that the Congress will soon consider legislation to grant this authority to FERC, and I thank Chairman Boucher for his initiative on this issue.

Finally, I believe the subcommittee's oversight has established much needed accountability in both the public and private sectors. For instance, as a result of our investigation into cyber attacks of Chinese origin, the inspector general, the Office of Security, and the FBI are busy conducting their own reviews of attacks on DHS systems. The contractors responsible for securing these systems also remain under investigation. This would not have happened without the oversight of this committee, and I hope that the public will soon hear about the findings of these reviews.

After providing misleading or confusing statements to this subcommittee in May, the North American Electric Reliability Organization has demonstrated a new commitment to cybersecurity, and they should be commended for their efforts thus far. After our hearing, NERC announced a process to create new standards for cybersecurity and created a new position of chief security officer for the electric grid. I was glad to see NERC endorsed the FERC emergency authority legislation last week, and look forward to watching their continued progress on this issue.

I also at this time want to take the opportunity to thank my partner and Ranking Member, Congressman Mike McCaul of Texas, who has been a true ally in this effort.

We have done some good work so far, but there is obviously much more work ahead of us. That is why we are here today. In October 2007, Mike and I were named co-chairs of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. The CSIS Commission is a nonpartisan commission composed of approximately 30 renowned cybersecurity experts, both in and out of Government from across the country. It is an impressive, experienced, and diverse group of people, and we are glad to be joined today by three members of the Commission: Jim Lewis, the program director; retired General Harry Raduege, one of the four co-chairs; and Paul Kurtz, also a member of the Commission. Unfortunately, Scott Charney, Vice President of Trustworthy Computing at Microsoft, and the other co-chair of the group, was unable to attend today, but he has been vital to the Commission's work. I want to acknowledge his contributions and leadership as well.

We are here to talk about what the next administration needs to do to improve cybersecurity. There are a number of significant issues that the incoming administration will face. New organization and national strategies must be considered, legal authorities altered and enhanced, investment and acquisition policies shaped, regulation and incentive regimes revised; and Government relationships with the private sector restored.

Congress plays a key role in the future of cybersecurity policy. Just as this administration hasn't spoken with one voice, however, committee jurisdictional squabbles threaten to divide the attention and focus of Congress on these issues as well. That is why I am announcing today that with my colleague, Ranking Member and partner in this effort, Congressman Mike McCaul and I created the first House Cybersecurity Caucus. The purpose of the Caucus is to raise awareness and provide a forum for Members representing different committees of jurisdiction to discuss the challenges in securing cybersecurity. We have already received great support from a number of Members, and we look forward to having our kick-off event in January 2009.

With that being said on the Caucus, I would like to, with unanimous consent, enter a letter into the record basically announcing and establishing the Caucus. Without objection, that will be so ordered.

[The information follows:]

**Congress of the United States**  
Washington, DC 20515

September 15, 2008

The Honorable Robert A. Brady  
Chairman  
Committee on House Administration Committee on House Administration  
1309 Longworth House Office Building  
Washington, D.C. 20515

The Honorable Vernon J. Ehlers  
Ranking Member  
Committee on House Administration Committee on House Administration  
1313 Longworth House Office Building  
Washington, D.C. 20515


Dear Chairman Brady and Ranking Member Ehlers,

We seek to establish the Congressional Cybersecurity Caucus. The purpose of this Caucus is to raise awareness and provide a forum for Members representing different committees of jurisdiction to discuss the challenges in securing cyberspace.

The Honorable James R. Langevin and the Honorable Michael T. McCaul will serve as co-chairmen of the Caucus. Jacob Olecott (202) 226-2623 and Deron McElroy (202) 226-8417 are the principal designated staffers who will work on the Caucus.

Sincerely,

  
James R. Langevin  
Member of Congress

  
Michael T. McCaul  
Member of Congress

PRINTED ON RECYCLED PAPER

Mr. LANGEVIN. With that, I just want to close by again thanking my partner in this effort, Congressman McCaul, and my fellow Members of the subcommittee for their participation, their support, and their efforts in this area. I want to thank of course the witnesses for their appearance here today. Your work on the CSIS Commission has been invaluable, and it is doing great service to our country, and particularly on the issue of cybersecurity. Again, I am grateful for your efforts.

With that, the Chair now recognizes the Ranking Member of the subcommittee, the gentleman from Texas, Mr. McCaul, for purposes of an opening statement.



Mr. McCAUL. Thank you, Mr. Chairman. We commend you for your excellent leadership, your steadfastness, your focus on such an important issue with regards to our national security. You have been a real leader in this Congress. I know this is our last hearing, but I know we will continue to work together as colleagues, as partners, and as friends on this important issue.

I think this Commission is a great legacy. When I look back at this Congress and all the things that we have accomplished, I can think of nothing that makes me more proud than the partnership I have had with you on cybersecurity and the creation of this important Commission. So I want to thank you for that.

Mr. LANGEVIN. Thank you.

Mr. McCAUL. You know, this issue doesn't always get the headlines. Sometimes people glaze over when you talk about it. But I think everybody sitting in this room understands the importance of it and how it impacts every facet of our lives, and how we are vulnerable to an attack either by criminals, by criminal enterprises, by espionage, or by cyber warfare. So this is a very, very important issue.

The oath we took coming into office was to protect and defend the Constitution from all enemies, foreign and domestic. The most solemn obligation we have as Members of Congress is to protect the American people. That is what this committee is all about, the Homeland Security Committee, and that is also what this Commission is about, is about protecting the American people.

I just came back from my district in my home State of Texas, where I witnessed a natural disaster bringing power down, destroying homes and lives amidst pain and suffering. That is a natural disaster. What we are talking about here is a force that would have the same potential, but it is man-made. So this committee protects the American people from both man-made and natural disasters.

So as we saw the power grids go down in the greater Houston area, the Texas Gulf Coast, a cyber attack could accomplish the same destruction by the click of a mouse. You know, over the last 2 decades America has become increasingly dependent on the smooth operation of our computer networks, and many critical sectors of our Nation's economy are dependent on cyberspace. It is clear that the security of the American homeland is directly tied to our cybersecurity efforts.

As this subcommittee under the Chairman's leadership has heard over and over again, our Nation is being attacked by determined enemies every single day in cyberspace, resulting in economic loss and the loss of critical information to hostile foreign powers. It is essential that the next administration place a high priority on cybersecurity. It is the intention of Chairman Langevin and myself to make sure it is high on the radar screen. The Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency has been working on a cybersecurity strategy since November 2007. That has been informed by many of this administration's current efforts to secure cyberspace. While the President's Comprehensive National Cybersecurity Initiative will help secure Government networks and help protect our Nation against computer network exploitation and attack, we also heard from a multitude of essential industry partners that without sub-

stantial private sector coordination, our networks will remain highly vulnerable.

I believe this Commission's report can and will add tremendously to the discussion on how to secure cyberspace and how to put the issue high on the next President—no matter which party—to put this issue high on the President's priority list.

A key component of the Commission's work has been the critical issue of how to involve the private sector in a truly comprehensive cybersecurity plan. While the work of the Commission is ongoing, we hope to hear from our witnesses today, and I hope to hear them discuss some of the Commission's work and roll out some of the preliminary findings and recommendations.

On a personal note, again I want to thank you, Chairman Langevin, for your truly bipartisan spirit. It is too bad that we in the Congress don't have more of that kind of partnering in a bipartisan way. I think that is what the American people want. I think it is what the American people deserve. When we can accomplish great things like this in a bipartisan way, I think it does the country tremendous service.

I want to thank the members that are here today from the Commission: Dr. Lewis, General Raduege, Mr. Kurtz. Mr. Powner, thank you for being here today from the GAO. But I feel like over the course of the last year or so that we have become good friends, and I believe that you all are doing some great work, and I look forward to hearing your testimony. Thank you.

Mr. LANGEVIN. I thank the Ranking Member for his statement, and again for his input and partnership in this effort. Before I go into introducing our panel today, I just want to for the record extend my sympathies, condolences to the people of Texas, for the loss that they have endured as a result of Hurricane Ike. We stand with you in solidarity and support in offering any help that we can give as you get through this difficult time. I know particularly your district was hit pretty hard. Again, our thoughts and prayers are with you and your district at this difficult time.

Mr. McCAUL. I appreciate it.

Mr. LANGEVIN. With that, I just wanted to say that other Members of the subcommittee are reminded that under the committee rules, opening statements may be submitted for the record.

[The statement of Hon. Brown-Waite follows:]

PREPARED STATEMENT OF HONORABLE GINNY BROWN-WAITE

Thank you, Chairman Langevin.

Thank you for holding this hearing today. As the country moves further and further into the twenty-first century, it will become increasingly important to improve and expand our ability to prevent and respond to cyber attacks. In the coming years, this committee, the intelligence community, the Department of Defense and the next administration will have to figure out the best way to move forward.

When a power plant in my State is attacked and shut down by a cyber attack from overseas, does the situation constitute an act of war or an act of terrorism? Will it be possible to discern the difference? Moreover, what is America's capacity to respond to such an attack?

Eighty percent of the information technology infrastructure in this country is owned and managed by the private sector. This fact alone means we will have to see greater cooperation between the private sector and the Federal Government when it comes to protecting our country from cyber attacks in the future. In addition, as the IT industry's largest single customer, I hope that the U.S. Government

can bring its size to bear in driving down costs and encouraging innovation in cybersecurity standards.

Finally, I would like to thank the witnesses for their efforts in preparing this study for the next administration. This will certainly be a priority going forward, and it seems clear that you have laid down some important groundwork.

I thank you for being here today, and I look forward to your testimony.

Mr. LANGEVIN. With that, I just want to now welcome our distinguished panel of witnesses.

Our first witness is Dave Powner, Director of Information Technology Management Issues at the Government Accountability Office. Mr. Powner and his team have produced a number of reports for this subcommittee in the 110th Congress. I want to take this opportunity to thank you and your team for your excellent work.

Our second witness is Jim Lewis, the Director of the Center for Strategic and International Studies Technology and Public Policy Program. He is a senior fellow. He is also the program manager for the CSIS Commission on Cybersecurity for the 44th Presidency. Jim, I want to welcome you here today and thank you for your friendship and leadership, particularly over this last year as the Commission has conducted its work. It has been outstanding.

Our third witness is General Harry Raduege. General Raduege is Chairman of the Joint Center for Network Innovation. Previously, he spent 35 years serving the Nation in the U.S. military. His latest assignments were Director of the Defense Information Systems Agency and Commander of the Joint Task Force for Global Networks Operations. General Raduege is also co-chair of the CSIS's Commission on Cybersecurity. Welcome.

Our fourth witness is Paul Kurtz, a partner at Good Harbor Consulting. Mr. Kurtz is a recognized cybersecurity and homeland security expert, having served in senior positions on the White House's National Security and Homeland Security Security Councils under Presidents Clinton and Bush. He is a member also of the CSIS Commission on Cybersecurity.

Welcome to all of you. For the purposes of opening statements, I have asked Mr. Lewis to deliver one opening statement on behalf of the other members of the CSIS Commission. Without objection, the witnesses' full statements will be inserted into the record. I will now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Powner. Thank you for being here today.

**STATEMENT OF DAVID POWNER, DIRECTOR, INFORMATION MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. POWNER. Chairman Langevin, Ranking Member McCaul. Members of the subcommittee, thank you for inviting us to testify on cybersecurity recommendations for the next administration. Also thank you for your oversight and leadership, as our work for you has resulted in numerous recommendations to DHS to improve the security of our Nation's cyber critical infrastructure.

Today we are releasing two new reports with significant recommendations, completed at your request, on cyber analysis and warning, and Cyber Storm exercises. My comments this afternoon will address key recommendations in these reports, as well as recommendations associated with organizational inefficiencies in leadership, sector-specific plans, and recovery planning.

Starting with organizational inefficiencies in leadership, several organizational issues need to be addressed to more effectively manage cyber operations at DHS. First, the National Communications System and the National Cyber Security Division need to integrate duplicative and overlapping operations to more efficiently respond to communication disruptions.

Next, the authorities and responsibilities associated with the new Cybersecurity Center, establishing a response to the President's January 2008 Cyber Initiative need to be reconciled with those of both the Assistant Secretary for Cyber Security and the NCSD. On a broader scale, a more fundamental policy issue that the new administration will need to tackle is whether these responsibilities should reside in DHS or whether the Nation's focal point for cyber should be elevated to the White House.

Over the course of our work, many in the private sector told us that it worked better when it resided there prior to the creation of DHS.

Next, sector planning. Mr. Chairman, we testified before you last October on the lack of cybersecurity focus in the 17 sector plans. The revised sector plans, which are expected by the end of the month, need to ensure that our Nation's key sectors are keenly focused on prioritizing cyber assets, conducting comprehensive vulnerability assessments, and addressing security weaknesses. Otherwise, this will remain a paper exercise.

A broader policy issue that the new administration should consider is whether all sectors are of equal importance, and whether our Nation should designate or prioritize certain sectors that are more critical.

Turning to cyber analysis and warning. Despite some progress, our report being released today shows that the US-CERT is far from the national cyber analysis and warning focal point envisioned in policy. Our report lays out 10 detailed recommendations and highlights 15 areas that need improved.

For example, US-CERT needs to expand its scope significantly, get more on the front end of attacks, be capable of handling multiple significant events, and issue warnings that are targeted, actionable, and timely. Leveraging similar capabilities at DOD and within the intelligence community should also be explored.

Next, recovery planning. Despite Federal policy requiring DHS to develop an integrated public-private plan to address internet disruptions, our representations to guide these efforts, and numerous congressional hearings on this, a joint public-private internet recovery plan still does not exist. Despite efforts with the various sectors, ISACs and coordinating councils to build better partnerships with the Government, this is a clear example of where the partnering has not been sufficient. Further, it leaves our Nation not fully prepared to respond to major internet disruptions.

The final area that I would like to address is cyber exercises. Today we are releasing a report where DHS has completed about two-thirds of nearly 70 actions called for from the 2006 Cyber Storm exercise. So, clearly, progress has been made and these exercises have proven useful.

However, Mr. Chairman, more aggressive follow-up needs to occur, and DHS needs to document lessons learned from these exercises more timely.

The March Cyber Storm. Two results are not to be documented until December of this year. Meanwhile, planning for the next exercise is underway. The Nation's focal point for cybersecurity should not and cannot be viewed as a slow-moving bureaucracy.

In summary, Mr. Chairman, I would like to thank you for your leadership and oversight of our Nation's cyber critical infrastructure protection and for focusing the next administration on these critical areas that need to be addressed.

Many large policy questions loom: organizational placement, continuing with the sector-based approach, regulation versus market incentives. However, no matter what decisions or approaches our Nation pursues, the Federal Government needs to do a better job in the areas it controls, including cyber analysis and warning, and coordinating exercises and recovery efforts so that it is viewed as a credible player and a partner in securing our Nation's critical infrastructure. Today it is not. We look forward to working with you in the future on these issues and to your questions.

[The statement of Mr. Powner follows:]

#### PREPARED STATEMENT OF DAVID POWNER

SEPTEMBER 16, 2008

#### GAO HIGHLIGHTS

Highlights of GAO-08-1157T, a report to Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives.

#### WHY GAO DID THIS STUDY

Recent cyber attacks demonstrate the potentially devastating impact these pose to our Nation's computer systems and to the Federal operations and critical infrastructures that they support. They also highlight that we need to be vigilant against individuals and groups with malicious intent, such as criminals, terrorists, and nation-states perpetuating these attacks. Federal law and policy established the Department of Homeland Security (DHS) as the focal point for coordinating cybersecurity, including making it responsible for protecting systems that support critical infrastructures, a practice commonly referred to as cyber critical infrastructure protection. Since 2005, GAO has reported on the responsibilities and progress DHS has made in its cybersecurity efforts. GAO was asked to summarize its key reports and their associated recommendations aimed at securing our Nation's cyber critical infrastructure. To do so, GAO relied on previous reports, as well as two reports being released today, and analyzed information about the status of recommendations.

#### WHAT GAO RECOMMENDS

GAO has previously made about 30 recommendations to help DHS fulfill its cybersecurity responsibilities and resolve underlying challenges. DHS in large part concurred with GAO's recommendations and in many cases has actions planned and underway to implement them.

#### CRITICAL INFRASTRUCTURE PROTECTION: DHS NEEDS TO BETTER ADDRESS ITS CYBERSECURITY RESPONSIBILITIES

#### WHAT GAO FOUND

GAO has reported over the last several years that DHS has yet to fully satisfy its cybersecurity responsibilities. To address these shortfalls, GAO has made about 30 recommendations in the following key areas.

## KEY CYBERSECURITY AREAS REVIEWED BY GAO

Area	
1. ....	Bolstering cyber analysis and warning capabilities.
2. ....	Reducing organizational inefficiencies.
3. ....	Completing actions identified during cyber exercises.
4. ....	Developing sector-specific plans that fully address all of the cyber-related criteria.
5. ....	Improving cybersecurity of infrastructure control systems (which are computer-based systems that monitor and control sensitive processes and physical functions).
6. ....	Strengthening DHS's ability to help recover from internet disruptions.

Source: GAO analysis.

Specifically, examples of what GAO reported and recommended are as follows:

- *Cyber analysis and warning.*—In July 2008, GAO reported that DHS's United States Computer Emergency Readiness Team (US-CERT) did not fully address 15 key cyber analysis and warning attributes. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. Consequently, GAO recommended that DHS address these attribute shortfalls.
- *Cyber exercises.*—In September 2008, GAO reported that since conducting a cyber attack exercise in 2006, DHS demonstrated progress in addressing eight lessons it learned from this effort. However, its actions to address the lessons had not been fully implemented. GAO recommended that the Department schedule and complete all identified corrective activities.
- *Control systems.*—In a September 2007 report and October 2007 testimony, GAO identified that DHS was sponsoring multiple efforts to improve control system cybersecurity using vulnerability evaluation and response tools. However, the Department had not established a strategy to coordinate this and other efforts across Federal agencies and the private sector, and it did not effectively share control system vulnerabilities with others. Accordingly, GAO recommended that DHS develop a strategy to guide efforts for securing such systems and establish a process for sharing vulnerability information.

While DHS has developed and implemented capabilities to address aspects of these areas, it still has not fully satisfied any of them. Until these and other areas are effectively addressed, our Nation's cyber critical infrastructure is at risk of increasing threats posed by terrorists, nation-states, and others.

Mr. Chairman and Members of the subcommittee: Thank you for the opportunity to join in today's hearing to discuss efforts in protecting our Nation's critical infrastructures from cybersecurity threats. The recent computer-based, or cyber, attacks against nation-states and others demonstrate the potentially devastating impact these pose to systems and the operations and critical infrastructures that they support.<sup>1</sup> They also highlight the need to be vigilant against individuals and groups with malicious intent, such as criminals, terrorists, and nation-states perpetuating these attacks.

Today, I will discuss the Department of Homeland Security's (DHS) progress in fulfilling its responsibilities to protect systems that support critical infrastructures—a practice referred to as cyber critical infrastructure protection or cyber CIP—as well as its progress in addressing our related recommendations. Due to concerns about DHS's efforts to fully implement its CIP responsibilities as well as known security risks to critical infrastructure systems, we added cyber CIP as part of our Federal information technology systems security high-risk area in 2003 and have continued to report on its status since that time.<sup>2</sup>

<sup>1</sup>Critical infrastructure is systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. There are 18 critical infrastructure sectors: agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, Government facilities, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, public health and health care, transportation systems, and water.

<sup>2</sup>For our most recent high risk report, see GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, DC: January 2007).

As requested, my testimony will summarize our key reports—two of which are being released today at this hearing—and their associated recommendations aimed at securing our Nation’s cyber critical infrastructure. Specifically, these reports and recommendations focus on: (1) Providing cyber analysis and warning capabilities; (2) being effectively organized to plan for and respond to disruptions on converged voice and data networks; (3) conducting and coordinating cyber attack exercises; (4) developing cyber-related sector-specific critical infrastructure plans; (5) securing control systems—computer-based systems that monitor and control sensitive processes and physical functions; and, (6) coordinating public/private planning for internet recovery from a major disruption.

In preparing for this testimony, we relied on our previous reports on Department efforts to fulfilling its cyber CIP responsibilities. These reports contain detailed overviews of the scope and methodology we used. We also obtained and analyzed information about the implementation status of our recommendations. We conducted our work, in support of this testimony, from August 2008 through September 2008, in the Washington, DC area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

#### RESULTS IN BRIEF

Since 2005, we have reported that DHS has yet to fully satisfy its cybersecurity responsibilities. These reports included nearly 30 recommendations on key areas essential for DHS to address in order to fully implement its cybersecurity responsibilities. Examples of what GAO reported and recommended are as follows:

- *Cyber analysis and warning.*—In a report being released today, we determined<sup>3</sup> that DHS’s United States Computer Emergency Readiness Team (US-CERT) did not fully address 15 key cyber analysis and warning attributes related to: (1) Monitoring network activity to detect anomalies; (2) analyzing information and investigating anomalies to determine whether they are threats; (3) warning appropriate officials with timely and actionable threat and mitigation information; and, (4) responding to the threat. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the Department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS agreed in large part with our recommendations.
- *Cyber exercises.*—In another report<sup>4</sup> being issued today, we concluded that since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing eight lessons it learned from these efforts. However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the Department identified 16 activities as ongoing and 7 as planned for the future. Consequently, we recommended that it schedule and complete all of the corrective activities identified so as to strengthen coordination between both public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation.
- *Control systems.*—In a September 2007 report and October 2007 testimony,<sup>5</sup> we identified that DHS was sponsoring multiple control systems security initiatives, including efforts to: (1) Improve control systems cybersecurity using vulnerability evaluation and response tools; and, (2) build relationships with control systems vendors and infrastructure asset owners. However, DHS had not established a strategy to coordinate the various control systems activities across Federal agencies and the private sector, and it did not effectively share information on control system vulnerabilities with the public and private sectors. Accordingly, we recommended that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information to improve Federal Government efforts to secure control systems governing critical infrastructure. DHS officials took our recommendations under advisement and more recently have begun developing a strategy, which is still a work in process. In addition, while DHS has

<sup>3</sup> GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, DC: July 31, 2008).

<sup>4</sup> GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned From Its First Cyber Storm Exercise*, GAO-08-825 (Washington, DC: Sept. 9, 2008).

<sup>5</sup> GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, DC: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08-119T (Washington, DC: Oct. 17, 2007).

begun developing a process to share sensitive information, it has not provided any evidence that the process has been implemented or that it is an effective information sharing mechanism.

#### BACKGROUND

The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. In recent years, the sophistication and effectiveness of cyber attacks have steadily advanced.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and nation-states. As we reported<sup>6</sup> in June 2007, cybercrime has significant economic impacts and threatens U.S. national security interests. Various studies and experts estimate the direct economic impact from cybercrime to be in the billions of dollars annually. In addition, there is continued concern about the threat that our adversaries, including nation-states and terrorists, pose to our national security. For example, intelligence officials have stated that nation-states and terrorists could conduct a coordinated cyber attack to seriously disrupt electric power distribution, air traffic control, and financial sectors. In May 2007, Estonia was the reported target of a denial-of-service cyber attack with national consequences. The coordinated attack created mass outages of its Government and commercial Web sites.<sup>7</sup>

To address threats posed against the Nation's computer-reliant infrastructures, Federal law and policy establishes DHS as the focal point for cyber CIP. For example, within DHS, the Assistant Secretary of Cyber Security and Communications is responsible for being the focal point for national cyber CIP efforts. Under the Assistant Secretary is NCSD which interacts on a day-to-day basis with Federal and non-Federal agencies and organizations (e.g., State and local governments, private-sector companies) regarding, among other things, cyber-related analysis, warning, information sharing, major incident response, and national-level recovery efforts. Consequently, DHS has multiple cybersecurity-related roles and responsibilities. In May 2005, we identified, and reported on, 13 key cybersecurity responsibilities called for in law and policy.<sup>8</sup> These responsibilities are described in Appendix I.

Since then, we have performed detailed work and made recommendations on DHS's progress in fulfilling specific aspects of the responsibilities, as discussed in more detail later in this statement.

In addition to DHS efforts to fulfill its cybersecurity responsibilities, the President in January 2008 issued HSPD 23—also referred to as National Security Presidential Directive 54 and the President's "Cyber Initiative"—to improve DHS and the other Federal agencies' cybersecurity efforts, including protecting against intrusion attempts and better anticipating future threats.<sup>9</sup> While the directive has not been made public, DHS officials stated that the initiative includes steps to enhance cyber analysis related efforts, such as requiring Federal agencies to implement a centralized network monitoring tool and reduce the number of connections to the internet.

#### DHS NEEDS TO ADDRESS SEVERAL KEY AREAS ASSOCIATED WITH ITS CYBERSECURITY RESPONSIBILITIES

Over the last several years, we have reported that DHS has yet to comprehensively satisfy its key cybersecurity responsibilities. These reports included about 30 recommendations that we summarized into the following key areas that are essential for DHS to address in order to fully implement its cybersecurity responsibilities.

<sup>6</sup>GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, DC: June 22, 2007).

<sup>7</sup>Computer Emergency Response Team of Estonia, "Malicious Cyber Attacks Against Estonia Come from Abroad," April 29, 2007, and Remarks by Homeland Security Secretary Michael Chertoff to the 2008 RSA Conference, April 8, 2008.

<sup>8</sup>GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, DC: May 26, 2005); *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, DC: July 19, 2005); and *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity*, GAO-06-1087T (Washington, DC: Sept. 13, 2006).

<sup>9</sup>The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, DC: Jan. 8, 2008).



## KEY CYBERSECURITY AREAS REVIEWED BY GAO

Area	
1. ....	Bolstering cyber analysis and warning capabilities.
2. ....	Reducing organizational inefficiencies.
3. ....	Completing actions identified during cyber exercises.
4. ....	Developing sector-specific plans that fully address all of the cyber-related criteria.
5. ....	Improving cybersecurity of infrastructure control systems.
6. ....	Strengthening DHS's ability to help recover from internet disruptions.

Source: GAO analysis.

*Bolstering Cyber Analysis and Warning Capabilities*

In July 2008, we identified<sup>10</sup> that cyber analysis and warning capabilities included: (1) monitoring network activity to detect anomalies; (2) analyzing information and investigating anomalies to determine whether they are threats; (3) warning appropriate officials with timely and actionable threat and mitigation information; and, (4) responding to the threat. These four capabilities are comprised of 15 key attributes, which are detailed in Appendix II.

We concluded that while US-CERT demonstrated aspects of each of the key attributes, it did not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtained information from numerous external information sources; however, it had not established a baseline of our Nation's critical network assets and operations. In addition, while it investigated if identified anomalies constitute actual cyber threats or attacks as part of its analysis, it did not integrate its work into predictive analyses of broader implications or potential future attacks, nor does it have the analytical or technical resources to analyze multiple, simultaneous cyber incidents. The organization also provided warnings by developing and distributing a wide array of attack and other notifications; however, these notifications were not consistently actionable or timely—providing the right information to the right persons or groups as early as possible to give them time to take appropriate action. Further, while it responded to a limited number of affected entities in their efforts to contain and mitigate an attack, recover from damages, and remediate vulnerabilities, the organization did not possess the resources to handle multiple events across the Nation.

We also concluded that without the key attributes, US-CERT did not have the full complement of cyber analysis and warning capabilities essential to effectively perform its national mission. As a result, we made 10 recommendations to the Department to address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS concurred with 9 of our 10 recommendations.

*Reducing Organizational Inefficiencies*

In June 2008, we reported<sup>11</sup> on the status of DHS's efforts to establish an integrated operations center that it agreed to adopt per recommendations from a DHS-commissioned expert task force. The two operations centers that were to be integrated were within the Department's National Communication System and National Cyber Security Division. We determined that DHS had taken the first of three steps towards integrating the operations centers—called the National Coordination Center Watch and US-CERT—it uses to plan for and monitor voice and data network disruptions. While DHS completed the first integration step by locating the two centers in adjacent space, it had yet to implement the remaining two steps. Specifically, although called for in the task force's recommendations, the Department had not organizationally merged the two centers or involved key private sector critical infrastructure officials in the planning, monitoring, and other activities of the proposed joint operations center. In addition, the Department lacked a strategic plan and related guidance that provides overall direction in this area and has not developed specific tasks and milestones for achieving the two remaining integration steps.

We concluded that until the two centers were fully integrated is completed, DHS was at risk of being unable to efficiently plan for and respond to disruptions to communications infrastructure and the data and applications that travel on this infra-

<sup>10</sup> GAO-08-588.

<sup>11</sup> GAO, *Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruption on Converged Voice and Data Networks*, GAO-08-607 (Washington, DC: June 26, 2008).

structure, increasing the probability that communications will be unavailable or limited in times of need. As a result, we recommended that the Department complete its strategic plan and define tasks and milestones for completing remaining integration steps so that we are better prepared to provide an integrated response to disruptions to the communications infrastructure. DHS concurred with our first recommendation and stated that it would address the second recommendation as part of finalizing its strategic plan.

DHS has recently made organizational changes to bolster its cybersecurity focus. For example, in response to the President's January 2008 Cyber Initiative, the Department established a National Cybersecurity Center to ensure coordination among cyber-related efforts across the Federal Government. DHS placed the center at a higher organizational level than the Assistant Secretary of Cyber Security and Communications. As we previously reported,<sup>12</sup> this placement raises questions about, and may in fact, diminish the Assistant Secretary's authority as the focal point for the Federal Government's cyber CIP efforts. It also raises similar questions about NCSD's role as the primary Federal cyber analysis and warning organization.

#### *Completing Corrective Actions Identified During A Cyber Exercise*

In September 2008, we reported<sup>13</sup> on a 2006 major DHS-coordinated cyber attack exercise, called Cyber Storm, that included large-scale simulations of multiple concurrent attacks involving the Federal Government, States, foreign governments, and private industry. We determined that DHS had identified eight lessons learned from this exercise, such as the need to improve interagency coordination groups and the exercise program. We also concluded that while DHS had demonstrated progress in addressing the lessons learned, more needed to be done. Specifically, while the Department completed 42 of the 66 activities identified to address the lessons learned, it identified 16 activities as on-going and 7 as planned for the future.<sup>14</sup> In addition, DHS provided no timetable for the completion dates of the on-going activities. We noted that until DHS scheduled and completed its remaining activities, it was at risk of conducting subsequent exercises that repeated the lessons learned during the first exercise. Consequently, we recommended that DHS schedule and complete the identified corrective activities so that its cyber exercises can help both public and private sector participants coordinate their responses to significant cyber incidents. DHS agreed with the recommendation.

#### *Developing Sector-Specific Plans That Fully Address All of the Cyber-Related Criteria*

In 2007, we reported and testified<sup>15</sup> on the cybersecurity aspects of CIP plans for 17 critical infrastructure sectors, referred to as sector-specific plans. Specifically, we found that none of the plans fully addressed the 30 key cybersecurity-related criteria described in DHS guidance. We also determined that while several sectors' plans fully addressed many of the criteria, others were less comprehensive. In addition to the variations in the extent to which the plans covered aspects of cybersecurity, there was also variance among the plans in the extent to which certain criteria were addressed. For example, fewer than half of the plans fully addressed describing: (1) A process to identify potential consequences of cyber attack; or, (2) any incentives used to encourage voluntary performance of risk assessments. We noted that without complete and comprehensive plans, stakeholders within the infrastructure sectors may not adequately identify, prioritize, and protect their critical assets. Consequently, we recommended<sup>16</sup> that DHS request that the lead Federal agencies, referred to as sector-specific agencies, that are responsible for the development of CIP plans for their sectors fully address all cyber-related criteria by September 2008 so that stakeholders within the infrastructure sectors will effectively identify, prioritize, and protect the cyber aspects of their CIP efforts. The updated plans are due this month.

<sup>12</sup> GAO-08-588.

<sup>13</sup> GAO-08-825.

<sup>14</sup> DHS reported that one other activity had been completed, but the Department was unable to provide evidence demonstrating its completion.

<sup>15</sup> GAO, *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-64T (Washington DC; October 31, 2007); and *Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*, GAO-08-113 (Washington DC; Oct. 31, 2007).

<sup>16</sup> GAO-08-113.

*Improving Cybersecurity of Infrastructure Control Systems*

In a September 2007 report and October 2007 testimony,<sup>17</sup> we identified that Federal agencies had initiated efforts to improve the security of critical infrastructure control systems—computer-based systems that monitor and control sensitive processes and physical functions. For example, DHS was sponsoring multiple control systems security initiatives, including efforts to: (1) Improve control systems cybersecurity using vulnerability evaluation and response tools; and, (2) build relationships with control systems vendors and infrastructure asset owners. However, the Department had not established a strategy to coordinate the various control systems activities across Federal agencies and the private sector. Further, it lacked processes needed to address specific weaknesses in sharing information on control system vulnerabilities. We concluded that until public and private sector security efforts are coordinated by an overarching strategy and specific information sharing shortfalls are addressed, there was an increased risk that multiple organizations would conduct duplicative work and miss opportunities to fulfill their critical missions.

Consequently, we recommended<sup>18</sup> that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information to improve Federal Government efforts to secure control systems governing critical infrastructure. In response, DHS officials took our recommendations under advisement and more recently have begun developing a Federal Coordinating Strategy to Secure Control Systems, which is still a work in process. In addition, while DHS began developing a process to share sensitive information; it has not provided any evidence that the process has been implemented or that it is an effective information-sharing mechanism.

*Strengthening DHS's Ability to Help Recovery From Internet Disruptions*

We reported and later testified<sup>19</sup> in 2006 that the Department had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for internet recovery. However, we determined that these efforts were not comprehensive or complete. As such, we recommended that DHS implement nine actions to improve the Department's ability to facilitate public/private efforts to recover the internet in case of a major disruption.

In October 2007, we testified<sup>20</sup> that the Department had made progress in implementing our recommendations; however, seven of the nine have not been completed. For example, it revised key plans in coordination with private industry infrastructure stakeholders, coordinated various internet recovery-related activities, and addressed key challenges to internet recovery planning. However, it had not, among other things, finalized recovery plans and defined the interdependencies among DHS's various working groups and initiatives. In other words, it has not completed an integrated private/public plan for internet recovery. As a result, we concluded that the Nation lacked direction from the Department on how to respond in such a contingency. We also noted that these incomplete efforts indicated DHS and the Nation were not fully prepared to respond to a major internet disruption.

In summary, DHS has developed and implemented capabilities to satisfy aspects of key cybersecurity responsibilities. However, it still needs to take further action to fulfill all of these responsibilities. In particular, it needs to fully address the key areas identified in our recent reports. Specifically, it will have to bolster cyber analysis and warning capabilities, address organizational inefficiencies by integrating voice and data operations centers, enhance cyber exercises by completing the identified activities associated with the lessons learned, ensure that cyber-related sector-specific critical infrastructure plans are completed, improve efforts to address the cybersecurity of infrastructure control systems by completing a comprehensive strategy and ensuring adequate mechanisms for sharing sensitive information, and strengthen its ability to help recover from internet disruptions by finalizing recovery plans and defining interdependencies. Until these steps are taken, our Nation's computer-reliant critical infrastructure remains at unnecessary risk of significant cyber incidents.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or Members of the subcommittee may have at this time.

<sup>17</sup> GAO-07-1036 and GAO-08-119T.

<sup>18</sup> GAO-07-1036.

<sup>19</sup> GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-06-863T (Washington, DC: July 28, 2006); and *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, DC: June 16, 2006).

<sup>20</sup> GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-08-212T (Washington, DC: Oct. 23, 2007).

## APPENDIX I

## DHS'S KEY CYBERSECURITY RESPONSIBILITIES

Responsibilities	Description of Responsibilities
Develop a national plan for CIP that includes cybersecurity.	Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including information technology and telecommunications systems (including satellites) and the physical and technological assets that support such systems. This plan is to outline national strategies, activities, and milestones for protecting critical infrastructures.
Develop partnerships and coordinate with other Federal agencies, State and local governments, and the private sector.	Fostering and developing public/private partnerships with and among other Federal agencies, State and local governments, the private sector, and others. DHS is to serve as the "focal point for the security of cyberspace."
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.	Improving and enhancing information sharing with and among other Federal agencies, State and local governments, the private sector, and others through improved partnerships and collaboration, including encouraging information sharing and analysis mechanisms. DHS is to improve sharing of information on cyber attacks, threats, and vulnerabilities.
Develop and enhance national cyber analysis and warning capabilities.	Providing cyber analysis and warnings, enhancing analytical capabilities, and developing a national indications and warnings architecture to identify precursors to attacks.
Provide and coordinate incident response and recovery planning efforts.	Providing crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cybersecurity continuity plans for Federal systems, planning for recovery of internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans.
Identify and assess cyber threats and vulnerabilities.	Leading efforts by the public and private sector to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies.
Support efforts to reduce cyber threats and vulnerabilities.	Leading and supporting efforts by the public and private sector to reduce threats and vulnerabilities. Threat reduction involves working with the law enforcement community to investigate and prosecute cyberspace threats. Vulnerability reduction involves identifying and remediating vulnerabilities in existing software and systems.
Promote and support research and development efforts to strengthen cyberspace security.	Collaborating and coordinating with members of academia, industry, and Government to optimize cybersecurity-related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies.
Promote awareness and outreach.	Establishing a comprehensive national awareness program to promote efforts to strengthen cybersecurity throughout Government and the private sector, including the home user.
Foster training and certification.	Improving cybersecurity-related education, training, and certification opportunities.
Enhance Federal, State, and local government cybersecurity.	Partnering with Federal, State, and local governments in efforts to strengthen the cybersecurity of the Nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States.

## DHS'S KEY CYBERSECURITY RESPONSIBILITIES—Continued

Responsibilities	Description of Responsibilities
Strengthen international cyberspace security.	Working in conjunction with other Federal agencies, international organizations, and industry in efforts to promote strengthened cybersecurity on a global basis.
Integrate cybersecurity with national security.	Coordinating and integrating applicable national preparedness goals with its National Infrastructure Protection Plan.

Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive—7, and the National Strategy to Secure Cyberspace.

## APPENDIX II

## KEY ATTRIBUTES OF CYBER ANALYSIS AND WARNING CAPABILITIES

Capability	Attribute
Monitoring .....	<ul style="list-style-type: none"> <li>—Establish a baseline understanding of network assets and normal network traffic volume and flow.</li> <li>—Assess risks to network assets.</li> <li>—Obtain internal information on network operations via technical tools and user reports.</li> <li>—Obtain external information on threats, vulnerabilities, and incidents through various relationships, alerts, and other sources.</li> <li>—Detect anomalous activities.</li> </ul>
Analysis .....	<ul style="list-style-type: none"> <li>—Verify that an anomaly is an incident (threat of attack or actual attack).</li> <li>—Investigate the incident to identify the type of cyber attack, estimate impact, and collect evidence.</li> <li>—Identify possible actions to mitigate the impact of the incident.</li> <li>—Integrate results into predictive analysis of broader implications or potential future attack.</li> </ul>
Warning .....	<ul style="list-style-type: none"> <li>—Develop attack and other notifications that are targeted and actionable.</li> <li>—Provide notifications in a timely manner.</li> <li>—Distribute notifications using appropriate communications methods.</li> </ul>
Response .....	<ul style="list-style-type: none"> <li>—Contain and mitigate the incident.</li> <li>—Recover from damages and remediate vulnerabilities.</li> <li>—Evaluate actions and incorporate lessons learned.</li> </ul>

Source: GAO analysis.

Mr. LANGEVIN. Thank you, Mr. Powner, for your testimony.

The Chair now recognizes Mr. Lewis to summarize the Commission's statement for 5 minutes. Welcome.

**STATEMENT OF JAMES A. LEWIS, PROJECT DIRECTOR, COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; ACCOMPANIED BY LIEUTENANT GENERAL HARRY D. RADUEGE, JR., CO-CHAIRMAN, COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; AND PAUL KURTZ, MEMBER, COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES**

Mr. LEWIS. I thank the committee for this opportunity to testify. Our goal is to identify actions that the next administration can take in its first hundred days to improve U.S. national security and global competitiveness.

In doing this, we would begin by noting that the next administration should build on the work of the comprehensive National Cybersecurity Initiative. It is a good start. Let me note that you, Mr. Chairman, and your colleague, Congressman McCaul, have provided invaluable support and guidance during the course of our work. I know a lot of times people say that, but I really mean it. It has really been a lot easier having you two. If I ever do another Commission, I want you to be on it. It has really helped. Your leadership has been crucial.

I would also like to note that we have received tremendous assistance from the Departments of Defense, Homeland Security, the intelligence community, and the FBI. So with all this help, it has been very valuable.

We are still working, as you noted. We hope to be done by November. But we are in a position where we can discuss some of our preliminary findings. I will begin by stating our two most important findings.

The first is that cybersecurity is now one of the most important national security challenges facing the United States. This is not a hypothetical challenge. We are under attack and we are taking damage.

Our second finding is that the United States is disorganized and lacks a coherent national strategy. Our recommendations call for the use of all instruments of U.S. power, diplomatic, military, economic, law enforcement, and intelligence, to secure cyberspace. This new strategy should be one of the first documents that the next administration issues.

We have looked at military activities in cyberspace. Most of these are classified. However, we will be able to discuss several important topics. The most important conclusion that we have reached regarding military activity is that credible offensive capabilities are necessary to deter potential attackers.

A comprehensive strategy for cyberspace creates an important challenge, however. We have found in our interviews and in our discussions that the ability to organize and coordinate Government activities for cybersecurity is inadequate. The central problems are lack of a strategic focus, overlapping missions, poor coordination, and diffuse responsibility. Our interviews have suggested that while DHS has improved in recent years, oversight of cybersecurity must move elsewhere.

We have considered many alternatives, such as whether it should be the intelligence community or DOD or other agencies. The conclusion that we have reached is only the White House has the authority needed for cybersecurity. This is not a call for a czar. Czars in Washington tend to be marginalized. Longing for a czar is a symptom of dissatisfaction with how our Government works now. One of the things we hope to do is develop recommendations for how to use technology to improve security and increase efficiency in Government.

On the subject of public-private partnerships, we found almost universal recognition that existing partnerships are not meeting the needs of either the Government or the private sector. Our work concentrated on two problems. The first is the need to rebuild trust. The second is to focus on infrastructures that are truly critical for cyberspace. For us those are the electrical power sector, telecommunications, and finance. We heard in many interviews that trust is the foundation of a successful partnership. We also heard that despite good intentions on all sides, trust between Government and the private sector has declined. Our recommendations will call for a restructuring to rebuild trust.

Our group had a long debate over the role of regulation and whether there has been market failure. Our conclusion is that greater regulation is necessary for critical cyber infrastructure, but the prescriptive command and control regulation will not increase security. Based on this committee's hearings with NERC and FERC, we are exploring new approaches to regulation.

We also concluded that cybersecurity requires better authentication. We know this is a sensitive subject, and we realize that any recommendation will need to ensure that privacy and confidentiality are protected. We heard many times in our interviews that key laws are outdated. The next administration, we will recommend, should work with Congress to revise investigative authorities, modernize Clinger-Cohen and FISMA, and remove the distinction between national security and civil agency systems found in many laws.

Our interviews suggest that the Federal Government can use its powers to change market conditions, it can increase resources available for cybersecurity by supporting training and education, it can expand research, it can encourage the deployment of more secure products and protocols. We will recommend that the new administration build on OMB's Federal Desktop Core Configuration and use Government and industry partnership to make better products for IT security.

Let me tell you what our next steps are. I hope you realize this was a cursory survey of where we are coming out in the Commission. There are other details that will come out in questioning. Our goal is to produce implementable recommendations that could guide both the legislative agenda and Presidential policy. We are on track to have this done by November.

Several difficult issues remain, including how to move from Industrial Age Government to one better suited to the Information Age, how to scope and design a new approach to regulation, where to locate authorities for cyberspace, and how to make public and private partnerships more efficient. I am confident that with your

help and guidance we can resolve these issues and offer recommendations to the next administration, the Congress, and the American people.

Thank you again for your support and for this opportunity. I look forward to your questions.

Mr. LANGEVIN. Thank you, Mr. Lewis, for your testimony.

[The statement of Mr. Lewis follows:]

PREPARED STATEMENT OF JAMES A. LEWIS

SEPTEMBER 16, 2008

I thank the committee for the opportunity to testify on the work of the CSIS Cybersecurity Commission on Cyber Security for the 44th Presidency. As you know, this Commission was established a year ago. It held its first meeting in November 2007. Our goal is to identify concrete actions that the next administration can take to improve cybersecurity. We are composed of forty individuals with extensive experience in cyber security and in Government operations, and our work has been supported by a number of eminent experts in this field. We have also received invaluable assistance from the Department of Defense, the intelligence community, the FBI and from elements of the Department of Homeland Security. Let me also note that you, Mr. Chairman, and your colleague Representative McCaul, have provided essential support and guidance during the course of our work. Your leadership has been crucial for shaping the report and in moving the Commission forward.

The starting point for the Commission's work was that the lack of cyber security and the loss of information were doing unacceptable damage to the United States. It has been 10 years since the first reports called attention to America's vulnerability in cyberspace. Unfortunately, the situation has gotten worse, not better, during the intervening decade. That cyberspace now provides the foundation for much of our economic activity is not readily apparent. However, those who wish to do harm to the United States have not failed to notice the opportunities created by the weaknesses of U.S. networks. There has been damaging losses of valuable information. These losses occurred in both the Government and the private sector, creating major risks for national security and doing major damage to U.S. global competitiveness. We are also deeply concerned by the idea that these intruders, since they were able to successfully enter U.S. networks to steal information without being detected, could just as well be leaving something behind, malicious software that could be triggered in a crisis to disrupt critical services or infrastructure.

I should note that when we began our work, the administration had not announced its National Cyber Security Initiative. We appreciate the willingness of some Departments to share the details of this highly classified activity to those of us who hold the appropriate clearances. As a group, we believe this initiative has begun to make a tremendous contribution to improving U.S. national security and we applaud those who are struggling to implement it. We have adjusted our work in light of the Initiative; it has brought progress, but there is still much work to be done.

The CSIS Cyber Commission hopes to have finished its work by November of this year. So our discussion today must necessarily reflect that in some instance, the group has not finished its work on key recommendations. What I and my colleagues can do, however, is brief the committee on the issues we have identified and some of the options we are considering.

Let me begin by noting our two most important findings. The first is that cyber security is now one of the most important national security challenges facing the United States. This is not some hypothetical catastrophe. We are under attack and taking damage. Our second finding is that the United States is not organized and lacks a coherent national strategy for addressing this challenge.

These two findings inform our work and our recommendations, and the Commission has identified several broad areas where we recommend that the next administration take immediate action. These are to develop a comprehensive national security strategy for cyberspace; to reorganize the governance of cyberspace to provide accountability and authority; to rebuild relationships with the private sector; to modernize cyberspace authorities; and use regulation and Federal acquisitions to shape markets.



## NATIONAL STRATEGY

In light of our conclusion that cyberspace must now be part of that national security strategy, our recommendations call for the use of all instruments of U.S. power to secure cyberspace. We identify five principle instruments—diplomatic, military, economic, law enforcement and intelligence—to achieve this and will recommend that the next administration make use of them in a coordinated and well-resourced national approach.

## DIPLOMATIC INITIATIVES

The diplomatic aspects of cyber security have been among the least developed elements of U.S. policy. Our vision of a diplomatic strategy involves advocacy, cooperation and norms. It is patterned after the U.S. experience in building international cooperation in non-proliferation. Increasingly, all nations and all peoples depend on cyberspace to conduct their daily affairs and this provides opportunities for cooperation. We will recommend that the United States advocate measures to secure cyberspace in every multilateral initiative where it is appropriate, just as we have advocated measures to advance nonproliferation or to combat terrorism.

## MILITARY AND DEFENSE

Much of the discussion of the military aspects of cybersecurity is necessarily classified. This limits what our Commission can say on offensive information warfare. However, we discussed several essential topics. These included how to improve deterrence, how to link strategy to an appropriate doctrine for use, and how to train and equip forces. The most important conclusion we reached is that credible offensive capabilities are necessary to deter potential attackers.

The United States has a doctrine for military operations in cyberspace, but we believe this doctrine will need to be expanded if it is to be effective. Doctrine provides guidance on the exercise of the various and overlapping legal authorities that apply to cyberspace, identifying when the use of law enforcement, military or intelligence authorities are appropriate. An expanded doctrine should specify relationships among agencies and lay out the decisionmaking process for various actions. Our initial conclusion is that the next administration should refine existing doctrine and create processes to work through the issues of deterrence and strategic operations in cyberspace.

## ECONOMIC TOOLS

Our review suggests that the United States would benefit from making greater use of the economic tools available to it. These tools include using international economic programs and organizations to promote cyber security, to develop norms and sanctions for international behavior, to work with international standards bodies and to invest in research and development in cybersecurity. A concrete example of this would be our bilateral trade negotiations with Russia. While the Russians had to improve their performance to many legal and trade requirements, they were not asked for better national performance in securing cyberspace. This must change.

## INTELLIGENCE AND LAW ENFORCEMENT

Our review of cybersecurity efforts found that the intelligence community has led the efforts to improve U.S. national cybersecurity. To foreshadow our discussion of organizational issues, we considered recommending that the intelligence community be formally given the lead role in securing cyberspace, but ultimately decided that this would be politically infeasible. Our recommendations emphasize that its primary role in securing cyberspace will be to support diplomatic, military, and domestic elements of a comprehensive strategy.

We were also impressed by the work of the Federal law enforcement community. Our recommendations will emphasize that an important activity for law enforcement is to work with other nations, as part of a larger diplomatic strategy, to shrink the “sanctuaries” available for cybercrime. Another essential law enforcement function is to ensure adequate protections for privacy and civil liberties in any cyber initiative. A comprehensive response to cyber attack need not come at the expense of civil liberties, and success will depend in some measure on the ability of the Government to assure Americans that their rights are being safeguarded. We believe this assurance requires a commitment from the White House and vigorous congressional oversight.

We believe that the new administration has an opportunity to build on the NCSI to create a coherent national strategy. This strategy should be one of the first policy documents that it issues. Moving to a strategy for cyberspace that focuses on using

all the tools of national power creates an important challenge however. We found that the current ability to organize and coordinate the use of diplomatic, military, economic, intelligence and law enforcement activities is inadequate. This will need to change improve cybersecurity.

#### ORGANIZATION

It did not take long for our group to conclude that our national efforts in cyberspace are disorganized. None of the existing cybersecurity structures are adequate. We found that the central problems in the current Federal organization for cybersecurity are the lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility. Much of the problem resides with the performance and capabilities of the Department of Homeland Security. While the Department's performance has improved in recent years, making this Department more effective will be an immediate task for the next administration. However, our view is that any improvement to the Nation's cybersecurity must go outside of DHS to be effective, and this will require rethinking the roles of DHS and the Homeland Security Council.

Given DHS's weaknesses, we considered a number of alternatives. The intelligence community has the necessary capabilities but giving it a lead role poses serious constitutional problems. DOD is well suited to manage a national mission, but giving it the lead suggests a militarization of cyberspace. We concluded that only the White House has the necessary authority and oversight for cybersecurity.

Simply appointing a czar, however, will not work. Czars in Washington tend to be either temporary or marginalized. Longing for a czar is a symptom of our industrial-age governmental organization. We are developing recommendations on how to leverage information technology to increase security while improving the efficiency, and transparency of Government operations. Our thinking on this has been shaped in part by the implementation of the Intelligence Reform and Terrorist Prevention Act, which imposed a new, more collaborative structure on the intelligence community. This is still a work in progress, but the IC's experience shows that the combination of a congressional mandate, adequate authorities, and a focus on "enterprise" solutions (e.g. those that cut across traditional agency barriers) can improve Federal performance.

We believe that the next administration's response to the cybersecurity challenge provides an opportunity to test new approaches to Federal organization that better leverage the use of cyberspace and social networking technologies to improve Government performance. It is time to move to an information-age Government. The Commission is considering several options for how best to achieve this. Our view is that this new model of governance must be based in the Executive Office of the President and make collaboration among agencies one of its missions.

#### PUBLIC-PRIVATE PARTNERSHIPS

The committee knows that the United States works with a variety of groups created to improve information sharing or build public-private partnerships. Based on a series of interviews, we found almost universal recognition that the status quo is not meeting the needs of Government or the private sector with respect to collaboration.

Our work concentrated on two problems that must be addressed if there is to be improvement. The first is to rebuild trust between the Government and the private sector. The second is to focus on infrastructures that are truly critical for cybersecurity—the sectors that provide the large national networks that create cyberspace—telecommunications, electricity, and finance.

We heard in numerous interviews that trust is the foundation of a successful Government/private sector relationship. We also heard that in the last few years, despite the profusion of advisory bodies and despite good intentions on all sides, trust between Government and the private sector has declined. Our recommendations will call for simplifying structure and building trust relationships. Information sharing, which drove much of the original thinking about how to work with the private sector, should become a secondary goal in our view.

#### REGULATION

Our group had a long debate over the role of regulation and whether there has been market failure in cybersecurity. Our conclusion is that greater regulation is necessary, but that prescriptive, command-and-control regulation will not produce a higher standard for security in critical cyber infrastructure. We are exploring a new approach to regulation that builds on and blends the strengths of the public and private sectors.

Based on this committee's hearings on NERC and FERC, we are exploring approaches that build on your vision of how NERC/FERC should work. This approach would task existing regulatory agencies for telecommunications, finance, and electrical power to devise regulations that embed cybersecurity requirements in a regulatory and compliance framework. To achieve this while avoiding the drawbacks of regulation, the Federal Government must find new ways to coordinate among agencies. We plan to recommend a "federated" approach to regulation that reduces the fragmentation and inconsistency found in cybersecurity regulation.

#### IDENTITY AND ATTRIBUTION

One of the new regulations we think are necessary for cybersecurity involve authentication of identity for critical infrastructures in cyberspace. The current internet is anonymous. Anonymity can preserve privacy and civil liberties, but it can also enable malicious behavior. We have concluded that the Government must require better authentication for critical infrastructure, and that this can be done in a way that protects privacy and confidentiality.

We started with the principle that unknown individuals or individuals using fraudulent identities should not be able to easily access critical infrastructure. We are developing a technology-neutral, "opt-in" approach to digital credentials for critical infrastructure, based on precedents from the work of the FDIC and the experience of the Department of Defense.

Our view is that it will be feasible to create a system where those who did not want to be authenticated could choose not to participate without penalty, but those who offer on-line services and wished to restrict them to authenticated individuals would not have that right denied to them. We recognize the sensitivity of any recommendation to require authentication and believe that no measure that does not adequately protect civil liberties will succeed, but we have concluded that security cannot be improved without better authentication of identity.

#### MODERNIZE AUTHORITIES FOR CYBERSPACE

We heard many times in our interviews that a legal structure that is a decade or two old ill-serves the Nation when it comes to cybersecurity. Some of this is due to transaction speed—an event in cyberspace may happen in seconds, but determining which authority to use in response can take hours or days (and we heard that the "default" authority is Title 3—law enforcement—as this is the set of authorities that is least likely to pose risks for civil liberties).

We believe that the next administration should work with Congress to revise three authorities: Title 3 investigative authorities related to cyberspace; the Clinger-Cohen Act and the Federal Information Security Management Act; and the distinction in law between national security and civilian agency systems currently embedded in many authorities. Revising existing authorities to serve the Nation effectively in cyberspace will be a complex legal operation that will require Congress and the new administration to work closely together, but it is an unavoidable challenge.

#### RESOURCES AND INCENTIVES

Our discussions and interviews suggest that the Federal Government has not made full use of its powers to change market conditions in ways that will improve cybersecurity. It can increase the inputs and resources available for cybersecurity by supporting training and education. It can expand and focus its investment in research. It can encourage the deployment of more secure products and protocols by using its purchasing power—the Federal Government does not have a dominant market share in IT, but it is the largest single customer for most IT products and it can use this to move the market in positive directions.

Our recommendations will call for changes in acquisitions requirements, collaborative work with companies on standards and best practices, and investment in human capital and in research to accelerate the rate at which we secure cyberspace. In this, we will recommend that a new administration build off OMB's Federal Desktop Core Configuration initiative.

Cooperation with private sector will be essential for success. Leveraging Government and industry partnerships can produce major improvements in security. Moreover, the development of more secure configurations must involve those international standards bodies who have been working in this area.

Our review suggests that the United States would benefit if it developed a national cyber education and training program. Our recommendation is that the United States develop an institutionalized program that establishes minimal standards for skills and knowledge sufficient to meet the cyber mission and enable attractive career paths.

The Federal Government is one of the largest purchasers of telecommunications services in the world—perhaps the largest. A Presidential mandate that the United States would only contract with telecommunications carriers that use DNS SEC would rapidly drive the market and provide benefits beyond the Federal Government. This recommendation is attractive because it could also be adopted by State and local governments.

#### INFORMATION ASSURANCE METRICS

A central part of any effort to judge whether a product or initiative has improved security is to identify or develop the metrics that can measure progress. There is no doubt that achieving compliance with best security practice is a basic foundation that is valuable and should be measured—what we lack is the ability to go beyond that with meaningful measures of security that inform the system owner on their actual risk profile, and how best to make intelligent investments in making the IT system more secure and reducing the overall risk.

#### ASSURING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY

Industrial Control Systems (also known as SCADA) are an integral part of electric power, oil, water, gasoline, chemicals, manufacturing, mining, transportation, food processing, etc. by providing control and safe shutdown of the processes for these facilities. Computer cyber vulnerabilities can affect the safe, functional performance of these systems and processes. We are working with experts in this field to develop recommendation on how to improve the security of ICS. These recommendations will probably be linked to our recommendation to develop a new regulatory approach for cyber security.

#### RESEARCH AND DEVELOPMENT FOR CYBERSECURITY

Although technology is only a part of the cybersecurity challenge, the next administration has an opportunity to use research and development to improve the security of computer and communications systems and the information created and stored within them.

Our initial work suggests that the United States needs a coordinated and strategic focus for Federal investments in cybersecurity R&D. Both basic research—often performed at universities and with benefits realized over the long term—and applied research—which uses existing technology to address near-term problems—must be part of this strategy. Just as the Department of Defense has successfully marshaled R&D to provide military advantage to the United States since the 1940's, the United States must harness R&D to America's cybersecurity needs.

One area we are considering for R&D involves re-engineering the internet, which operates with protocols written in the 1970's and 1980's. A simple analogy would be to ask if it is safe to drive a 30-year-old car that still uses its original equipment. WE believe it is time to upgrade. Many of outside experts suggested that we remember that cyberspace is a human construct and that the internet's architecture, with research and international cooperation, can be significantly improved. This is a bold and complex recommendation that will require a coordinated effort managed by the White House as part of a larger strategy, but it is not out of reach.

#### NEXT STEPS

The Commission's goal is a package of implementable recommendations that could help to guide both a legislative agenda and presidential policy documents. We are on track to have this done within the next 2 months. Several difficult issues remain, including how to move from an industrial age model of governance to one better suited for the information age, how to scope and design a new approach to regulation, where to locate the authorities for cyberspace within the Federal Government, and how to make public-private partnership more efficient. I am confident that with your help and guidance we can resolve these issues and offer our recommendation to the next administration, the Congress and the American public. Thank you again for this opportunity and I would be happy to take any questions you may have.

Mr. LANGEVIN. Before I go to questions, I just wanted to mention that there will be a continuation of today's hearing basically on Thursday, the same subject of the CSIS Commission's preliminary findings, that takes place on Thursday before the House Permanent Select Committee on Intelligence. I suspect that this hearing and the one on Thursday will be just the first of many, both on the

work of the CSIS Commission, but on cybersecurity overall as we head into the next Congress.

With that, I want to thank the witnesses for their testimony. I will remind each of the Members that they will have 5 minutes to question the panel. I will now recognize myself for questions.

Let me just start with a few general questions for the panel. Based on your professional judgment and knowledge of DHS's state of preparedness, are we adequately prepared for a major cyber attack? Is the U.S. Government effectively organized to meet that cybersecurity threat? Why has DHS struggled to fill its mission? Finally, should DHS lead the cybersecurity mission in the U.S. Government?

It is a general question for the panel, so whoever would like to—

Mr. POWNER. Mr. Chairman, based on the work we have done for you over the years, I think the short answer is that we are not prepared for major significant events, especially when you start looking at multiple events. I will point to a couple key bodies of work that we focused on. If you looked at a major internet disruption, are we prepared to really deal with a major internet disruption from a public-private point of view? No. If you look at the cyber exercises that have been conducted to date, there are a lot of lessons learned that have come out of those, a lot of basic things that still need to be in place: communications, how we involve law enforcement and those types of things. So we are not well prepared today.

Mr. LEWIS. I would agree with that, Mr. Chairman. We are not prepared. I think DHS has struggled, for a number of reasons. One of the most important is that it really doesn't have the authority to direct other departments and agencies. If anything, its authority has probably declined as other departments have moved out on this issue. So it is hard for us—I began in this effort by thinking that we should strengthen DHS. We did not receive much encouragement when we put that forward to either the experts we talked to, to people within Government, or to even members of my own Commission. So I was shot down by my own Commission.

Should it lead? There are things that only DHS can do, and it is appropriate to locate them there. We are in the process of trying to determine what those are. But our view, I think I speak for the Commission, is that many of these functions need to move to the White House. This is now a serious national security problem. It needs to be treated as such. It needs to be taken under the leadership of the National Security Council. So our view is while there are things DHS should do, cybersecurity now needs to receive White House attention.

General RADUEGE. I would just add, Mr. Chairman, that I believe in my travels I have heard numerous times other nations looking to the United States for leadership in cybersecurity strategy. I think that just underlines the fact that the internet is certainly a global network, and it has international proportions. So with what Dr. Lewis has just mentioned, I would add that we need an international focus on this. It is a national security issue, but it has international proportions.

Mr. KURTZ. Just to build on what others have said, as Jim pointed out, this is really no longer just a homeland security issue, it

is a national security issue. That is, if you will, a change significantly since DHS was stood up. Now we have espionage on a massive scale by our adversaries. That I think takes it really—much of the responsibility out of the hands of the Department of Homeland Security. That is not their fault.

However, point No. 2 is there really is no one in charge right now at DHS. That is why they have struggled. When you look across the spectrum at DHS, you have an Under Secretary, you have an Assistant Secretary for Policy. We have others that are supposedly working side-by-side, but really are not working side-by-side. It is as though you have several people with their hands on the steering wheel, and there is really no common direction as to which way to go.

Also, as General Raduege said, we have several other agencies that have assumed significant responsibilities. So someone has got to be in charge.

The final point is—and that we can't lose sight of in this reorganization—is how do we have someone in charge but still recognize that this is the information infrastructure we are talking about? So traditional command-and-control that we are used to seeing inside DOD and other places may not be the most appropriate way to go; that we need to establish better means of collaboration. That is one of the issues that the Commission has looked at.

Mr. LANGEVIN. Let me—it is probably a good segue into my next question—it is a known fact in Washington whoever controls the purse strings controls the mission. This might explain why DHS as the coordinating body has been so very unsuccessful in achieving goals and securing cyberspace. Who should have budget authority over the Federal Government's cybersecurity missions? Where should this authority lie? What role should OMB have?

We can just go right down the line again if you would like to have your input.

Mr. POWNER. Mr. Chairman, we look at and I look at the entire IT budget of the Federal Government, \$70 billion that we spend. In terms of authority, DHS does not have the purse strings, that is clear. The authority is dispersed. Then what happens not only in cybersecurity but in the whole IT arena is we don't have enough oversight on how that money is spent.

So I think going forward, consistent with some of the Commission's recommendations, we ought to look at creating organizations that control the purse strings as well as have the appropriate authorities moving forward.

Mr. LEWIS. Thank you, Mr. Chairman. That is a good question. It is one that we struggled with in the Commission. I am sure that people at OMB will be happy to know that we moved the budget authorities all around the Federal Government for a while, and I don't think we have quite figured out where to put them.

What I will say, though, is I think the sense of where we are coming out is that, you know, OMB has to be the place that coordinates budgets. That is what they do for the President. But we do need somebody that provides oversight, coordination, collaboration among Federal agencies. This is also a White House function, but not an OMB function.

So what we are suggesting is that when it comes to budget functions, keep them at OMB. When it comes to policy functions, move them somewhere into the White House. We are looking at a number of suggestions on where that should be. But currently OMB kind of acts in both a policy role and a budget role, and we think it is time to focus them on their budget responsibilities.

Mr. LANGEVIN. Are you suggesting that OMB would ultimately have veto power over policy since they control the budget, or how would that work?

Mr. LEWIS. I think we want it to work more like other agencies. So if I can use the example of the work that has been done to reform the intelligence community; which is, you have a new figure at the top of the different agencies in the intelligence community, the Director of National Intelligence. That director coordinates the budget for all those agencies and then works with OMB to come up with the President's submission to Congress.

So I think what we are looking for is something that will reach across all the agencies but continue the pattern we have now. Some of the reasons we are suggesting that is only for practical reasons. OMB has the expertise. They have the oversight of the whole budget. It can work in other agencies such as Defense or the intelligence community when they are strong. So I think, create the strong entity and this will not be an issue.

General RADUEGE. I would say that the example of Director of National Intelligence is new. I believe we have seen areas, as Dr. Lewis has mentioned, that have brought new insight and perspective to 16 formerly intelligence community activities that were acting without an overseer. I think there has been good progress made to establish common priorities and common direction across the 16 independent intelligence activities with the DNI oversight.

Mr. KURTZ. Just to add on once again to what has been said, the question of OMB is a bit complicated when it comes to information systems because it is not only the budgetary authority they have, but it is, if you will, the authority they have under FISMA to set policy on information systems. So that gives them a little bit of a different edge than we find in many other situations. I think that situation needs to be reconciled.

The Commission may well come out that the FISMA-related authorities of OMB maybe need to be pulled out and placed into another—placed into another entity perhaps associated with the White House.

When it comes to the budget-related issues, though, the ODNI model is good, but I would offer two other similar models, and that is the drug czar, where the drug czar had, if you will, oversight of the budget, could put together specific programs, make sure agencies were adequately funding them.

Similarly, that was done in the case of counterterrorism, informally. When I was in the White House and we got into counterterrorism-related budgets, when we saw agencies that weren't necessarily doing enough, we would go directly to OMB and to the agencies and say we really needed to bolster these programs. It worked fairly effectively when we had proper support from others in the West Wing.

Mr. LANGEVIN. Thank the panel for their answers to those questions. The Chair now yields to the Ranking Member for 5 minutes for questions.

Mr. MCCAUL. Thank you, Mr. Chairman, thank you again for your great leadership, as I mentioned in my opening statement.

I agree, Mr. Kurtz, it is no longer just a homeland security issue, this is a national security issue that doesn't really know borders. There are no borders to cyberspace. It is international in its scope. We have seen the vulnerabilities in terms of shutting down power grids, the financial sectors, the aviation sectors, the potential damage that could be done.

I see my good friend and colleague Al Green has joined us, representing the Houston area. We have seen first-hand how the natural disasters I mentioned in my opening statement have caused tremendous damage, destruction, loss of human life. This is again a man-made threat.

In our hearings the one thing that seemed like a common theme was that no one—who is in charge was the question. Even though I think we tried to relegate a lot of that authority to DHS, the authority wasn't direct. The coordination has not been where we would like it to be. Certainly, with respect to the DOD and the NSA, you have such great expertise in this area in terms of the operations side. We didn't see the coordination that I frankly would have liked to have seen better coordination between those who know how to do this offensively on the operations side and those who need to do this defensively to protect the United States.

Let me just add to this as well just the massive intrusions that we have seen in the Federal networks and the amount of information, data that has been stolen. I would like to know how these recommendations will help prevent that type of intrusion that we have seen more in the form of espionage. The cyber warfare issues arise.

Let me say also that I am very pleased with these recommendations in terms of putting somebody that has the President's ear in charge of this, so it elevates this to the Presidential level. I think that has been somewhat lacking. I think that will provide the coordination necessary between all these relevant agencies.

How we do that, whether it is in the NSC or putting an office in the Executive Office of the President, I think all those are very good ideas that I know you are entertaining and have put forth. How do these make us safer?

Then, General Raduege, you talked, I thought very importantly, about the international focus. What is the vehicle, what would be the vehicle for coordinating with other countries that we believe to be friendly? There are a lot of countries that aren't friendly to us that are trying to get this technology offensively.

General RADUEGE. Thank you for that question, Mr. McCaul. As I have traveled and talked to other leaders in other Nations, they are looking for answers in preparing their own cybersecurity strategies. So a simple question that they would ask me was who should we come to talk to in the United States that we can talk with about your overarching strategy for protecting cyberspace? That was a very difficult question, because I reflected on the number of activities and bodies and organizations that have a piece. But there



was never one place that I could recommend that they go to talk to to get the overarching view that you would work, initially at least, across international borders. So there was no one individual who had the perspective of the entire national perspective and strategy over the United States.

So that is why our recommendations of our Commission was to have someone that really could speak as the authority, and with the President's ear, to know that what we were telling other Nations as far as our priority of this very important activity is at the Presidential level, and this is where you can get your answers, and this is the kind of strategy that we have, and let's work together across borders, national borders, in securing cyberspace as a global capability for all of us.

Mr. MCCAUL. Thank you, General Raduege.

Dr. Lewis, you said we are not prepared today. I tend to agree with that assessment to some extent. With respect to the private sector, that is a tremendous challenge. I think your words were we need to restore the trust. I agree the sharing of the information and the coordination with the private sector has not been where it needs to be, I think, to adequately protect this country.

The idea of sharing information is a difficult one. After 9/11, we had sharing of information between the intelligence side, the law enforcement side, the breaking down the walls of communication, you know, enhancing communications. You run into some problems with the private sector. I wanted to get your input from the Commission's recommendations on how to most effectively enhance that coordination and sharing of information.

Two major hurdles. One is when you are dealing with the intelligence community you have clearances and you have classified information. Second, a private entity, a business, is going to be reluctant to share with the Federal Government information, and particularly information regarding vulnerabilities within their company that they have witnessed, without adequate protection that that will not get somehow leaked or be accessible to some sort of requests from the Federal Government. How do you propose to overcome those or meet those challenges and overcome those hurdles?

Mr. LEWIS. Thank you. We had a long series of discussions with many people involved in the current partnerships organizations. We also talked with several of the leaders of the British Center for the Protection of National Infrastructure on how they do public-private relationships. We talked with a number of companies that aren't involved. So we did a lot of interviews on this, and we did hear some common messages.

I think where we came out was, first, you need to restructure. You know, there are groups, ISACs, SECs, these have a function in supporting DHS. They don't do what we need to do in cybersecurity. So we are recommending thinking of changing that a little bit. The first thing, drawing on the experience of the NSTAC, which General Raduege was involved in, drawing on the experience of the British with CPNI, drawing on some earlier U.S. initiatives. We think you need to develop a Presidential-level advisory body, maybe something like the President's Export Council, like the NSTAC, senior-level figures who come regularly, who meet with

senior-level people in the administration who have the clearances, who exchange information, and, because this is a long-term relationship, build trust. You need that relationship for trust. We used to have that before some functions moved to DHS. Through no fault of its own, that trust is no longer there. So we think this is one of the things that needs to go back to the White House.

The other issue—and we are struggling with it a little bit—is, as you noted, companies don't like to share information if they think it is revealing something to their competitors or if they are giving the Government something and never get anything back. We think you need a new kind of organization that fixes both those problems, something that we have been calling an operational organization. When companies run into problems they do collaborate, right? But they collaborate informally now. They don't do it through the existing structures.

So we are looking for a way to capture that informal collaboration, to create affinity groups around a particular problem, and then use that as the vehicle to drive an operational approach.

In both of these cases, though, the new senior-level advisory body and the new operational body, information sharing would be a tool. It wouldn't be the goal. Information sharing seemed really important after 9/11. Now I think we recognize it is just one way to achieve our mission, which is to secure the Nation's networks more comprehensively.

Mr. MCCAUL. All right. I like the creativity in trying to deal with this. If I could just indulge the Chair for one more question. With respect to regulations, that always certainly raises a lot of issues. But this new concept is not a mandate, a prescriptive type of regulation. Can you expand on what this new concept would be with respect to any sort of regulatory scheme coming out of these recommendations?

Mr. LEWIS. Certainly. Let me walk you through where we are and note that we haven't reached the end of the path. So if I end abruptly, please excuse me. But we had a discussion: Can we rely on the market? After some back-and-forth, we decided no, that you needed to have some additional regulation.

We then decided, though, this isn't national regulation or broad regulation. You don't need to give DHS the authority to regulate cyberspace. That is unnecessary. There are in the three critical infrastructures we identified—telecom, finance, electricity—existing regulatory authorities. I should note we have depended in many ways on the work GAO has done on this. The study they are releasing today has been very helpful in guiding us. So our recommendations will change somewhat as we work through the new material they have provided.

In those three structures, though, you have plenty of regulatory bodies. They have some authority. What they don't have is a way to coordinate or a way to figure out if what they are doing is adequate. So what we would like is for some new entity, probably in the White House, to be able to provide an approach that finds, you know, common things that agencies can do with their regulated sectors to find sort of minimal thresholds for security, and that finds a way to build collaboration. So we are looking to do this in as light a manner as possible.

Command-and-control regulation, I think we have all agreed prescriptive regulation will not work. But at the same time, as you discovered in your NERC/FERC hearings, just giving the companies their head and saying, "Good luck and write back when you have something to tell" is also insufficient. So we are hoping we can come up with what we have been calling an ideal NERC/FERC approach. I know after the hearing, both NERC and FERC have gone off and are trying to redo how they approach this problem. We are learning from them. So that is what we are looking at.

Mr. MCCAUL. Well, thank you very much. Just let me close by saying thank you to the three members of the Commission and all the members of the Commission who provided such a great public service to this Nation. Thank you.

Mr. LANGEVIN. I thank the gentleman. The Chair now recognizes the gentleman from New Jersey for 5 minutes.

Mr. PASCRELL. Thank you, Mr. Chairman. Mr. Chairman, it is interesting that the GAO presentation and report by the Commission, although not finished yet, are pretty close. Interesting. There is no national strategy, which would mean to me we are waiting for the politick to take into effect. We are still at risk in this area. We lack a specific focus. I think those were your words, Dr. Lewis.

Mr. LEWIS. Yes.

Mr. PASCRELL. So I have some comments to make and then I have some questions. I think that let's be real, Mr. Chairman. This administration has been a disaster when it comes to cybersecurity since 2003 when they got rid of Richard Clarke. It has been all downhill since. It wasn't until the DNI came into effect last year and started shaking things up that they showed any initiative whatsoever.

So let's name names and let's talk about accountability, because I think that we have been so concerned about being politically correct, that is why we haven't corrected the vulnerability. We are good at it, both sides of the aisle. This is not partisan. The last time I checked, we have at least four people over at DHS who claim to be in charge of cybersecurity.

Dr. Lewis, I want you to interrupt me if I say anything that is not true. Just interrupt me.

Mr. LEWIS. You are on track so far.

Mr. PASCRELL. It is no wonder that we are in the shape we are in today. Robert Jamison, the Under Secretary who leads the ship, apparently, gave himself a solid C in cybersecurity last time he came before the full committee.

Mr. Chairman, when was getting a C a good mark? I know what the nuns used to tell me. You are on the way to D. You remember, Mr. Chairman, that shortly after, the chief information officer told us, "You don't know what you don't know." That is rather startling. He was promoted to Deputy Under Secretary. These are the individuals in charge of cybersecurity in DHS.

Now, the White House has been equally fill-in-the-blank. They announced a new initiative and then overclassified everything. The Senate tried for months to get them to make the information public so we could have a public dialog about some of these things. The White House naturally refused to budge. Then yesterday I see that the Special Assistant to the President is giving a talk about the

Nation's cybersecurity posture. I don't know if you heard it or read it. They had the gall to charge Government employees \$50 to attend it to hear this guy talk.

Now, a lot of things have been said about New Jersey, but there has got to be some transparency here as to what in God's name is going on. To hear about an initiative that they refused to talk about for months.

I am hoping that Mr. Kurtz, who was Special Assistant to the President when he worked for Richard Clarke, and the other panelists might have some insight for us about this sad state of affairs.

So let me ask all of you, from your dealings with these people, these folks who I named—I gave you names—is cybersecurity an issue of national security that is being taken seriously or is it simply a political football that people are trying to build a legacy out of? Who wants to take the first crack?

Mr. LEWIS. I will go first. You know, in some ways I am going to defend the administration a little bit, which would probably be a surprise to them.

We had a lunch with Admiral McConnell shortly before he was confirmed as the Director of National Intelligence. At that lunch somebody asked him: What is the one thing that keeps you up at night? You know, I thought he was going to say Iraq or North Korea. He said cybersecurity. I was shocked. So he at least has been focused on this from the time he took office. I give him credit for that.

The Comprehensive National Cybersecurity Initiative is actually a very useful series of steps. It is doing the TIC, EINSTEIN, the FDCC. Some of the other activities have made some useful progress. One of the things I know people are worried about, one of the things we want to help with in the Commission is not to have a fumble. You know, we have made a little progress in the last year. When the administration changes the norm, whether it is a Democratic or a Republican administration, you know, is to sort of start over. We can't afford that.

So we want to say some of the things that have come out of this initiative have been good. I agree with you completely, it would be a lot easier to avoid that fumble if this wasn't classified Top Secret.

I think yesterday's presentation by a series of administration figures was useful. I understand in part that was in reaction to the hearing today and a way to get some information out. So you can take credit for that. But I think they have done some good things. We do have a lot of work to do, I couldn't agree with you more. But there are folks who are trying.

Mr. PASCRELL. General.

General RADUEGE. Thank you, sir. To answer your questions, I believe there are people who are taking this issue very seriously. I believe, though, that they are frustrated, as I talk with them individually in social settings and professional settings, of how massive this issue really is. They are frustrated with their organizations, they are frustrated with where this issue lies in their organization, at what level, and the processes that are involved with trying to coordinate actions for a national-level serious issue with the patchwork and the centers of brilliance, but also the centers of incom-

petence that are throughout the daily workings and dealings that they are faced with.

Mr. PASCRELL. Thank you. Mr. Kurtz.

Mr. KURTZ. Let me try to answer by a bit of a story first. Back at the end of June, DHS convened a meeting to discuss Project 12, which is, if you will, the one element of the initiative that relates to the private sector. At the head of the table we had several senior people from the Department of Homeland Security, including Under Secretary Jamison, Secretary Baker, Secretary Garcia, and Admiral Brown.

What was so discouraging about that day, and it was a day that I will never forget—and I worked in Government for a long period of time, but it was really a travesty—we had in-fighting between the DHS senior leadership as to how to proceed. It demonstrated in spades the lack of leadership, the fact that no one was in charge at DHS. What was really sickening about it was that we had probably 70 or so people from the private sector there who have spent a lot of time over the past several years trying to work with the Department, and yet again had been asked to put together some material for the Department to digest on how they could work together, but the Department basically threw it overboard, wasn't listening to the private sector. That was incredibly discouraging to witness.

I will say Admiral Brown sat at that meeting, saw what happened, and I think has been trying to work a way forward. So I don't want to implicate Admiral Brown in this at all.

The second point is I do find it also very discouraging that it took so long for the White House to come out and speak about this publicly. Even when they did, it was in kind of a strange manner, having an event at an association, whereas it wasn't, if you will, a public event.

What is really discouraging, taking all of that into account, is the Comprehensive National Cyber Initiative is actually not bad. It was a good-news story for the White House. It was a good-news story for the administration. But they sought to overclassify, to make it political, to see that CSIS was only out to go after them, when in the end, CSIS, Jim Lewis, John Hamre, opened the door to several agencies to come in and brief, and they took us up on that. DOD, the DNI, FBI, NCIS all came to brief us. Elements of DHS came to brief us. Not all. The White House in all cases discouraged people from participating.

Mr. PASCRELL. Why?

Mr. KURTZ. You ask them. I don't know the answer.

Mr. PASCRELL. That is a good answer. Okay.

Mr. LEWIS. Can I add one thing too, too, sir? We all three of us still have our clearances. All three of us have worked on very highly classified programs. All three of us have gotten briefed on the Cybersecurity Initiative. There is no reason to classify it. We know what classified programs look like. There are a couple parts in this that, yeah, they are classified. But most of it, it could be open.

Mr. PASCRELL. I think the Chairman is noting this. How about Mr. Powner?

Mr. POWNER. Clearly, our work over the years has showed that DHS has been completely ineffective in fulfilling their responsibil-

ities as the cybersecurity focal point. I want to just—and you know, we see this a lot where everyone points fingers and we don't have authority and the whole bit. Executives get paid to break down the bureaucracy and get things done. That hasn't happened.

Mr. PASCRELL. Thank you, Mr. Powner.

Thank you very much. Mr. Chairman. I want to hang a question out there, and I don't want an answer. I want us to think about it very seriously, though. If we are attacked in cyberspace, therefore, what level of response is appropriate?

Thank you, Mr. Chairman.

Mr. LANGEVIN. Thank the gentleman for his questions. The gentleman from Texas, Mr. Green, has 5 minutes for questions.

Mr. GREEN. Thank you, Mr. Chairman. I am not sure exactly where to go after all that I have heard. I thank all of you for taking the time to be a part of trying to assist your Government, and for your candor. I will tell you we don't hear this type of straightforward talk, straight talk, if you will, that often. I appreciate the fact that you have been absolutely candid about this.

I am going to go in a slightly different direction, although I have enjoyed hearing concerns about who should be in charge. In your review of this, did you conclude that the technology does exist to actually have cybersecurity?

Mr. LEWIS. The short answer would be yes. Now, people would be surprised at that. You can never secure things 100 percent, just as your car can never be 100 percent safe. But there is a lot we could do. There are things where spending on research would help, but we have not taken advantage of all of the technology that is available.

Mr. GREEN. Yes, sir.

Mr. KURTZ. Well, I would agree with what Jim is offering. There are lots of interesting technologies out there that can be deployed, and there are some questions as to where they are most effectively deployed in order to better protect the networks, in other words, at the edge or in the core. That is one of the issues we are, in fact, wrestling with in the area of regulation, as to what might carriers or ISPs—what should they consider doing in order to better protect the networks?

So the technologies exist. But, however, rubbing up against that is the open nature of the internet and anonymity on the internet. In these two, the desire to be secure, the desire to have private communications, and at the same time use the same vehicle for anonymous communications, they conflict. That is an issue that, at least over the past 48 hours in the e-mail going back and forth among commissioners, is a real issue to seek to try to find a way forward on. It is not clear.

Mr. GREEN. Yes, sir.

General RADUEGE. I would just say, Congressman, that the technology definitely exists, but it always has to be refreshed.

In this particular area of information technology and the speed that the internet and all of our information networks work at and the sophisticated attackers that we have out there and those who are always trying to gain some advantage, the technology has to keep up as they gain in their ability to do evil to us, whether it

is in the areas of national security perspectives or in cybercrime or even the eventuality of perhaps terrorist activity.

Mr. POWNER. What we see in our work is primarily an issue with—not with the technology but with individuals; do we have cyber analysts, criminal investigators, and those types of expertise in the Federal agencies such as DHS and other places.

Mr. GREEN. Hence, is it fair to conclude—and I suspect that this has already been stated—but if the technology exists, and we are still at an unacceptable level of vulnerability, then it is clearly a question of leadership?

Yes, sir.

Mr. KURTZ. Yes, it is a question of leadership. It is also a question of putting in place the mechanisms to promote collaboration, if in the space of just the Federal Government, in securing its own networks, is putting in place the collaboration mechanisms.

Actually, the Comprehensive National Cyber Initiative envisions some of that. Unfortunately, as far as execution on the initiative, one of the key centers associated with that, the National Cyber Security Center has, if you will, not been able to proceed because it has not received adequate funding in support. So it is struggling. Similarly, the US-CERT, which has responsibilities in this area, is struggling as well.

So it is, if you will, not just technology. It is putting the organizations together with the right technology and collaboration mechanisms in order to achieve better security.

Mr. GREEN. On the question of leadership—and I know that is a very broad statement, leadership, and I understand it—should this leadership emanate with the Congress? Or should we continue to allow the executive to prescribe, mandate which Department, who is going to be in charge? Or do you think that we need to, here in Congress, give some additional sense of direction, if you will?

Mr. KURTZ. Well, I think, first, the effort by Chairman Langevin and a call to establish a caucus, a cyber caucus, here in the House at least, is a very good idea. Because I think, in working on this issue in the past, there are several committees of jurisdiction up here on Capitol Hill, and trying to get everybody on the same page and come up with a common waveform is difficult.

At the same time, if Congress could do that, then I think there could be, if you will, more focused direction from Capitol Hill as to where the executive branch might ultimately focus. But I think the executive branch, for its part, should and can reorganize itself to have more authority and oversight within the EOP, the Executive Office of the President.

Mr. LEWIS. It is strange, in following on Paul's remarks, Congress has to be involved in this. One of the things we have concluded is that it won't work unless you have both Congress and the executive branch. What we need is vigorous oversight, which this committee has provided. We have seen how useful it can be, but we need more of it. We need the right authorities. People mentioned FISMA, Clinger-Cohen, some other authorities, Title 3, Title 18. We have authorities that were very often written in the 1970's. Only Congress can update them to fit the age we live in now.

You know, and finally we need the right level of funding. Congress has been so far in cybersecurity. In fact, you have been gen-

erous ahead of knowing what the plans were to spend the money, so I congratulate you on that. It is a first. But we do need Congress to continue to support building the infrastructure that will let us be more secure.

So these are things that neither branch can do by themselves, and we have to find a way to build the partnership between you two for this to work.

Mr. GREEN. Thank you, Mr. Chairman.

Just a closing comment. Given the comments that have been made, we have some duty to respond. Hopefully we will find a way to get that done, because the vulnerability being offset by the technology, and if that doesn't occur, and then we do have an attack, obviously people are going to want to know why we didn't do more.

Thank you.

Mr. LANGEVIN. I thank the gentleman for his questions, as well as his final statement. I agree, there is no issue that is as important right now as cybersecurity. As we go forward, it poses a significant national security challenge to the United States, not just now but well into the future, particularly because it is such a moving target. We are going to have to try to continue to stay one step ahead of those who may wish us harm. This is not a partisan issue, and we need to stay united and well-coordinated on the effort to have a comprehensive cybersecurity strategy as we go forward.

With that, I will have just one final question, and then I am going to yield to the Ranking Member for a closing comment as well.

Since this administration is coming to an end and there will be a new administration coming in, we are just now starting to really have a comprehensive, coordinated response and strategy on cybersecurity for the 21st century and for the 44th presidency.

Can I ask the panel, have you studied the Presidential candidates' platforms? What they are proposing in terms of cybersecurity? What efforts will the Commission make to place its report on the desk of the new administration?

I will leave that for the panel, whoever would like to begin first.

Mr. LEWIS. I will start, Mr. Chairman.

We have been working with the campaigns. We have kept them informed from the start of the Commission. There are several people on the Commission involved in both campaigns.

When we began this, we picked three campaigns as the ones likely to make it to the finish line. Of the two that are there, they were among the three we picked. So we do have contacts.

We hope and have reached out to both of the campaigns now to have more detailed briefings, briefings with more senior members of each campaign. We waited, on your recommendation, I might add, for the conventions. Now that the conventions are over, we have asked, can the Chairman go and brief on our recommendations? So I think in the next month or so, we will have that opportunity.

Mr. LANGEVIN. Very good.

General RADUEGE. I would say, Mr. Chairman, that I have been encouraged by both candidates in the fact that they have both recognized cybersecurity in their statements and needing greater investment and greater attention, and the fact that it appears like



they both recommend that this be a top priority in their administration.

Mr. LANGEVIN. Very good.

Mr. Kurtz, anything to add in closing?

Mr. KURTZ. No, that is fine.

Mr. LANGEVIN. Okay. Very good.

With that, I will yield to the Ranking Member for a comment.

Mr. McCAUL. I thank the Chairman.

You know, as I look at the pictures of the World Trade Center behind the witnesses, and the Pentagon, you know, associating myself with Congressman Green's remarks, we don't want to be sitting here some day with a cyber 9/11 and say, what could we have done differently to stop that from happening? I think that is the whole vision of this commission and the value of this commission.

There are some very good men and women serving at the Federal level and serving in our military and serving at NSA and serving at DHS, who sincerely want to protect this Nation. I believe there are many that are doing a fine job. This commission is not in the business, in my view at least, it was not my vision that this commission would be in the business of finger-pointing and partisanship. In fact, what we attempted to do—this is one of the rare times that I have seen, frankly, that we have been able to come together, I think. The beauty of it is coming together in a bipartisan way, with a nonpartisan commission that is simply just trying to protect America. I think that is the value that the next administration and the next President will see in this and, I think, the American people.

Thank you.

Mr. LANGEVIN. Very good. I thank the Ranking Member for his comments.

I just want to thank the panel again for their testimony today, particularly for the great work that the GAO has been doing over the years. Thank you for your contributions and service to this subcommittee in particular.

I want to thank the members of the CSIS Commission who are here today for your great leadership, dedication. You, as well, perform a great service to our Nation. We are all grateful for your dedication, your patriotism and for the countless hours that you put into this effort to better secure the Nation against cybersecurity attack and just cybersecurity in general.

So, with that, I want to again thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the subcommittee may have additional questions for the witnesses, and we will ask that you respond expeditiously in writing to those questions.

Again, we remind everyone that this will be one of many hearings that will take place going forward. The next hearing will be before the House Permanent Select Committee on Intelligence that will occur on Thursday.

Hearing no further business, the subcommittee now stands adjourned.

[Whereupon, at 3:40 p.m., the subcommittee was adjourned.]